Universal Chosen-Ciphertext Attack for a Family of Image Encryption Schemes

Junxin Chen, Lei Chen, and Yicong Zhou, *Senior Member, IEEE*

***Abstract*—In recent decades, there has been considerable popularity in employing nonlinear dynamics and permutation-substitution structures for image encryption. Three procedures generally exist in such image encryption schemes: the key schedule module for producing encryption elements, permutation for image scrambling and substitution for pixel modification. This paper cryptanalyzes a family of image encryption schemes that adopt pixel-level permutation and modular addition-based substitution. The security analysis first reveals a common defect in the studied image encryption schemes. Specifically, the mapping from the differentials of the ciphertexts to those of the plaintexts is found to be linear and independent of the key schedules, permutation techniques and encryption rounds. On this theory basis, a universal chosen-ciphertext attack is further proposed. Experimental results demonstrate that the proposed attack can recover the plaintexts of the studied image encryption schemes without a security key or any encryption elements. Related cryptographic discussions are also given.**

***Index Terms*—Cryptanalysis, substitution and permutation, modular addition, chosen-ciphertext attack.**

I. Introduction

BENEFITING from fascinating Internet applications such as Twitter and Instagram, recent years have witnessed dramatic popularity of multimedia exchange over public networks. This popularity further leads to increasing requirements for secure transmission and storage of multimedia data over public communication infrastructures. Encryption is the easiest method for dealing with this issue. Obviously, conventional encryption schemes such as DES (data encryption standard) and AES (advanced encryption standard) are straightforwardly applicable for encrypting multimedia data by considering it as a standard bitstream. This is the so-called 'naive encryption' [1]. Many researchers strive for specialized image encryption by leveraging the intrinsic features of multimedia data, such as adjacent pixel correlations and large data volumes. The encryption schemes analyzed in this paper belong to the latter. Image encryption schemes are the primary concern of this work since they generally act as foundations for frame-by-frame video encryption [2].

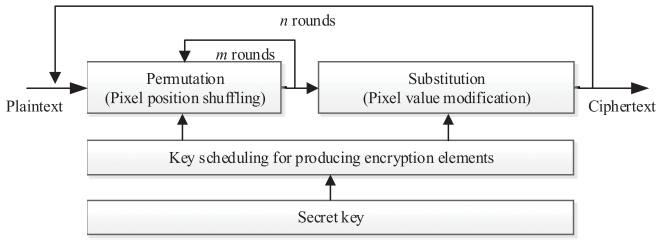


Fig. 1. Permutation-substitution architecture for image encryption.

The permutation-substitution[1] network is the most popular architecture for image encryption. As plotted in Fig. 1, a permutation process is implemented for pixel shuffling (with their values unchanged), and then a substitution procedure is performed for modifying pixel values and obtaining avalanche performance [3], [4]. The encryption kernel repeats over many rounds to achieve a higher security level. In the literature, chaos and other nonlinear dynamics have been frequently employed to produce the encryption elements required for permutation and substitution. This is because the fundamental properties of chaotic systems, such as ergodicity and sensitivity to initial conditions, are desirable for confusion and diffusion effects [1]. In recent decades, the permutation-substitution structure has aroused a boom in image encryption schemes. The primary innovations of image encryption schemes can be identified in three categories: novel permutation approaches [4]–[13] and new substitution techniques [4], [11], [14], [15] and more complex dynamic phenomena [11], [14]–[21].

Generally, statistical tests are introduced for the security assessment of the permutation-substitution image encryption schemes mentioned in the previous paragraph. The performance indicators include histogram, adjacent pixel correlation, information entropy, NPCR (number of pixel changing rate), UACI

Manuscript received December 1, 2019; revised July 10, 2020; accepted July 13, 2020. Date of publication July 24, 2020; date of current version July 30, 2021. This work was supported by the National Natural Science Foundation of China under Grants 61802055 and 61771121, in part by the Fundamental Research Funds for the Central Universities (N2019001), in part by China Postdoctoral Science Foundation (2019M660511), in part by the Science and Technology Development Fund, Macau SAR (File no. 189/2017/A3), and in part by the University of Macau (File no. MYRG2018-00136-FST). The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Abdulmotaleb El Saddik. *(Corresponding author: Yicong Zhou.)*

Junxin Chen is with the College of Medicine and Biological Information Engineering, Northeastern University, Shenyang 110004, China, and with the Key Laboratory of Intelligent Computing in Medical Image, Ministry of Education, Shenyang 110004, China, and also with the Department of Computer and Information Science, University of Macau, Macau 999078, China (e-mail: chenjx@bmie.neu.edu.cn).

Lei Chen is with the Nsfocus Information Technology Co., Ltd, Beijing 100089, China, and also with the Research Institute of Information Technology (RIIT), Tsinghua University, Beijing 100084, China (e-mail: clei@bupt.edu.cn).

Yicong Zhou is with the Department of Computer and Information Science, University of Macau, Macau 999078, China (e-mail: yicongzhou@um.edu.mo).

Color versions of one or more of the figures in this article are available online at https://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TMM.2020.3011315

[1]It may be referred to as permutation-diffusion in some studies.

(unified averaged changed intensity), and the NIST (National Institute of Standards and Technology) randomness test. However, Preishuber *et al.* [2] found that these empirical indicators are not powerful conditions for security declarations. Actually, many permutation-substitution image encryption schemes that have passed these tests were cracked [22]–[26]. Relative cryptanalysis achievements usually focus on a specific encryption scheme. For example, the equivalent permutation key of Fridrich's [3] scheme was recovered by a chosen-ciphertext attack [22], [23], while Li *et al.* [26] cryptanalyzed an image encryption scheme that employed the first-order time-delay system. Generalized attacks of permutation-only [27]–[29] and substitution-only [30] encryption schemes were conducted without considering the mutual security promotion of the permutation and substitution modules. Few universal cryptanalyses for iterative permutation-substitution image encryption schemes have been reported.

This paper moves one step further. The 'generalized cryptanalysis,' 'permutation-substitution' and 'iteratively performed' are all considered. These parameters are the initial motivations and innovations of this work. Specifically, this paper cryptanalyzes a family of permutation-substitution image encryption schemes. From the outside, they possess the following similar features.

1) Both the permutation and substitution modules are included.
2) The encryption core, i.e., permutation-substitution network, can be iteratively performed with round keys.
3) Image permutation is performed at the pixel level with an individual permutation vector.
4) Substitution is implemented using a modular addition technique, including Eqs. (1) to (3) or their variants. In these equations, $c(i), m(i)$, and $k(i)$ refers to the ciphertext, plaintext and the substitution mask, respectively, $c(i-1), c(i-2)$ represents the previous encrypted pixels, and the operator $\dot{+}$ denotes the modular addition operation.

$$c(i) = m(i) \dot{+} k(i) \tag{1}$$

$$c(i) = m(i) \dot{+} k(i) \dot{+} c(i-1) \tag{2}$$

$$c(i) = m(i) \dot{+} k(i) \dot{+} c(i-1) \dot{+} c(i-2) \tag{3}$$

Typical image encryption schemes can be found in [10]–[12], [14], [19], [31]–[34], which all fall into the scope of this work. Theoretical analysis first finds that these encryption schemes have a common vulnerability. Specifically, the mapping from the differentials of the ciphertexts to those of the plaintexts is revealed to be linear and independent of the permutation technique, employed nonlinear dynamics, encryption rounds and round keys. On this basis, a chosen-ciphertext attack is further proposed to crack all of them without any modification.

This work is different from [2], whose emphasis focuses on the insufficiency of the widely adopted statistical/empirical tests for security declaration. This paper will theoretically illustrate and experimentally verify that a family of permutation-substitution image encryption schemes is breakable. This work can also be considered as the inheritance and development of related works [25], [35], [36], whereas our mathematical analysis and universal practicability are better than these counterparts.[2] There are four distinct advantages of the proposed attack. First, our attack method is universal for cracking a family of image encryption schemes rather than a specified scheme. This universality is guaranteed by the theoretical analysis. Second, the studied image encryption schemes include both permutation and substitution, and the encryption kernel can be iterated for many rounds. Third, the proposed attack's complexity is independent of the encryption iterations and round keys. Finally, the proposed attack can recover the plaintexts without knowledge of the security key or any encryption elements.

Our contributions are summarized as follows.

1) This paper cryptanalyzes a family of image encryption schemes that adopt pixel-level permutation and modular addition-based substitution.
2) The security defect of these image encryption schemes is mathematically formalized.
3) A chosen-ciphertext attack is proposed, which can crack this family of image encryption schemes without any modification.
4) It is further revealed that the security of the studied image encryption schemes cannot be improved by either employing complex chaotic systems, applying sophisticated permutation techniques, or increasing the encryption iterations with round keys.
5) The proposed chosen-ciphertext attack is experimentally validated.

The remainder of this paper is organized as follows. Section II reviews the related works. From a basic model, Section III derives the concerned security drawback and then proposes a chosen-ciphertext attack. Application of the proposed attack to break the studied image encryption schemes is analyzed in Section IV, while the experimental results are given in Section V. Finally, Section VI concludes the paper.

II. Related Works

A. Notations

Unless otherwise indicated, most of the notations adopted in this paper are listed in Table I.

Examples or complementary descriptions are as follows:

- Generally, $\boldsymbol{M}$ and $\boldsymbol{C}$ denote the plaintext and ciphertext in an encryption scheme, and P and D specifically refer to the intermediate ciphertexts in a permutation-then-substitution or substitution-then-permutation scheme, respectively. The notations W and K represent the permutation vector and substitution matrix.
- The image is assumed to have a size of $H \times W$. This paper prefers the vector representation of an image, i.e., $\boldsymbol{M} = \{m(1), m(2), \ldots, m(i), \ldots, m(L)\}, L = H \times W$.
- For the superscript and subscript, for example, $\boldsymbol{C}_1^{(1)}$ is the ciphertext of $\boldsymbol{M}_1$ in the first round of encryption,

[2]For example, the attack in [25] requires mathematical generalization, while the security analysis in [35] should better be extended to more encryption rounds.

TABLE I
SUMMARY OF THE ADOPTED NOTATIONS

Notation	Style	Description
A	capital	a constant
$\boldsymbol{X}$	bold uppercase	an assembly, generally denotes a vector
$x(i)$	lowercase	i^{th} element of corresponding assembly in bold uppercase
$\boldsymbol{X}^{(i)}$	superscript bracket-within-number	factors in the i^{th} encryption round
$\boldsymbol{X}_i$	subscript	index of factors
$\dot{()}$	algebraic operators with a dot on the head	modulo algebra as described in the following equations, where G represents the gray level of the plaintext's pixel. $a\dot{+}b = (a+b) \bmod G$ $a\dot{-}b = (a-b) \bmod G$ $a\dot{\times}b = (a\times b) \bmod G$ $\dot{\sum}_{i=1}^{j} a(i) = a(1)\dot{+}\ldots\dot{+}a(j)$

whereas $\boldsymbol{P}_2^{(3)}/\boldsymbol{D}_2^{(3)}$ denotes the intermediate permutation/substitution ciphertext of $\boldsymbol{M}_2$ in the 3^{rd} iteration.

- As special cases, $\boldsymbol{M}^{(1)} = \boldsymbol{C}^{(0)}$ is the input plaintext, and the output ciphertext is denoted as $\boldsymbol{C}^{(Out)} = \boldsymbol{C}^{(N)}$, where N refers to the iteration counts of an encryption scheme.
- The modular subtraction of two images is defined as their differential, denoted as $\Delta\boldsymbol{M} = \boldsymbol{M}_1\dot{-}\boldsymbol{M}_2$.

B. Overview of Image Encryption Schemes

Since the standardization of permutation-substitution architecture [4], a boom in image encryption schemes has aroused [37]. Their innovations can be identified in the following three primary categories.

1) *Novel permutation approaches:* There are two types of permutation techniques. The first type treats image pixels as a whole rather than splitting them into binary streams in advance. Cat map and Baker map are the most popular permutation techniques, and they have been employed in the foundation work of Fridrich [3]. In addition, Chen *et al.* [4] extended the cat map to three dimensions, while a general gray code has also been exploited for image shuffling [5]. Instead of pixel-by-pixel shuffling, row and column circular permutation [38] as well as block shuffling techniques have been developed [6]. Other mathematical transforms were also introduced, for example, quaternion rotation [7], Hilbert curve [8] and many others [9], [10], [13]. Bit-level permutation is implemented by splitting the plain image into a binary matrix so that the bit relocation and pixel value modification effects are simultaneously obtained [39].
2) *New substitution techniques:* Algebraic operations are always employed for pixel substitution. Typical substitution equations are listed in Eqs. (1)–(3) and (4)–(5). The operator $\oplus$ represents bitwise exclusive-OR (XOR) in Eqs. (4)–(5)[3]

$$c(i) = m(i) \oplus k(i) \oplus c(i-1) \tag{4}$$

$$c(i) = (m(i)\dot{+}k(i)) \oplus k(i) \oplus c(i-1) \tag{5}$$

In addition, various substitution patterns are also attractive, such as joint compression-encryption systems [40], [41], bilateral substitution [42], simultaneous permutation substitution [43], [44] and pixel-related avalanche mechanisms [45].
3) *Introducing complex dynamic phenomena:* The permutation vector and substitution masks are secret essentials in these encryption schemes. They are generally secretly and randomly produced. In early development, classical chaotic systems such as logistic maps and cat maps have been frequently adopted. However, they were assumed to be insecure in recent years. As replacements, hyperchaotic maps [16] and various improved chaotic systems [11], [14], [17]–[19] were introduced to generate the required encryption elements. In addition, other complex dynamics originating from physical phenomena also show great potential. For example, a quantum walk was executed in [15], [20], while Wang *et al.* [21] introduced Brownian motion to produce key stream elements.

A comprehensive review of the application of nonlinear dynamics for image encryption can be found in [37], [46], [47].

C. Overview of Cryptanalysis Works

According to the Web of Science, 196 related publications were found.[4] They generally conducted the security analysis first, and then an implementable attack was followed. The state-of-the-art cryptanalysis works have been reviewed in [46], while a brief review is given here.

1) *Most of them are case specific:* In other words, the majority of the published cryptanalysis achievements are only valid for their specified image encryption schemes and will become infeasible for other encryption schemes. Fridrich's [3] encryption scheme was cryptanalyzed in [22], [23], which demonstrated a chosen-ciphertext attack for retrieving the permutation matrix. The encryption scheme employing a first-order time-delay system was recently broken by Li *et al.* [26] through a chosen-plaintext attack, and Wang *et al.* [24], [25] cryptanalyzed two bit-level encryption schemes.
2) *Cryptanalyzing permutation-only and substitution-only image encryption schemes:* In [27]–[29], a permutation cipher has been generalized to an invertible key-dependent vector $W = [w(i) \in \mathbb{L}], \mathbb{L} = \{1, 2, \ldots, L\}$. Particle $w(i)$ refers to the secret coordination of a plain pixel that is

[3]Note that this paper focuses on cryptanalyzing a family of image encryption schemes that adopt pixel-level permutation and modular addition-based substitution. The image encryption schemes using Eqs. (4)–(5) for substitution are outside of the scope of this work.

[4]Search '(attack OR cryptanalysis OR breaking OR cracking OR (security analysis) OR cryptanalyzing OR comment) AND image AND (cipher OR cryptosystem OR encryption)' in the title domain of Web of Science, Date 24/11/2019.

relocated to the i^{th} position in the ciphertext.[5] as indicated in Eq. (6). The function $\mathcal{W}$ is further defined to generalize the permutation encryption, as given in Eq. (7). Known-plaintext and chosen-plaintext attacks have been proven feasible for recovering the permutation vector.

$$p(i) = m(w(i)) \tag{6}$$

$$P = \mathcal{W}(\boldsymbol{M}) \tag{7}$$

In addition, Zhang *et al.* [30] attacked image encryption schemes that merely use substitution methods. However, practical image encryption schemes usually include both permutation and substitution modules. The generalized cryptanalysis of permutation-only and substitution-only encryption schemes [27]–[30] was illuminative, whereas it was not feasible for the encryption schemes combining permutation and substitution.

3) *Cryptanalyzing a popular substitution mechanism within a single round:* As mentioned above, Eqs. (1)–(5) are the most popular pixel substitution mechanisms. They have frequently been employed in permutation-substitution image encryption schemes. Under the assumption of known-plaintext and chosen-plaintext attacks, Zhang *et al.* [35] analyzed the security of Eq. (5). However, this cryptanalysis assumed that the encryption was implemented in only a single round and will become invalid for the iterative structure. In contrast, practical image encryption schemes are generally proposed to be iteratively implemented with round keys, such as AES.

III. Problem Formulation and the Proposed Attack

A. A Basic Encryption Model

The basic encryption scheme is constructed according to the studied permutation-substitution structure depicted in Fig. 1. This basic model generalizes the studied image encryption schemes, independent of the employed permutation techniques and chaotic systems. Previous works have exploited area-preserving maps [3], [4] or some mathematical transforms [7], [8] for image shuffling and developed more complex dynamics [14] for pixel substitution. However, a permutation vector and a substitution mask matrix are sufficient for generalizing the encryption effects of the employed permutation and substitution particulars.

Considering the i^{th} round of the basic encryption model, the image shuffling process is generalized as a permutation vector $W^{(i)}$, while the substitution mask is denoted as $K^{(i)}$. Thus, the permutation product is obtained as $P^{(i)} = \mathcal{W}^{(i)}(\boldsymbol{M}^{(i)})$, and the ciphertext is produced according to $\boldsymbol{C}^{(i)} = P^{(i)} \dot{+} K^{(i)}$. The permutation and substitution operations are iteratively implemented for N rounds to produce the final ciphertext. The basic encryption scheme is finalized as

$$\begin{cases} C^{(Out)} = \boldsymbol{C}^{(N)} \\ \boldsymbol{C}^{(i)} = \mathcal{W}^{(i)}(\boldsymbol{M}^{(i)}) \dot{+} K^{(i)} \\ \boldsymbol{M}^{(i)} = \boldsymbol{C}^{(i-1)} \\ \boldsymbol{C}^{(0)} = \boldsymbol{M}^{(1)} \end{cases}. \tag{8}$$

B. Security Analysis

Assume that there are two plaintexts $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$ and their ciphertexts $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ in a certain encryption round. Referring to Eq. (8), the differential of the ciphertexts is obtained as

$$\begin{aligned} \Delta\boldsymbol{C} &= \boldsymbol{C}_1 \dot{-} \boldsymbol{C}_2 \\ &= (\mathcal{W}(\boldsymbol{M}_1) \dot{+} K) \dot{-} (\mathcal{W}(\boldsymbol{M}_2) \dot{+} K). \\ &= \mathcal{W}(\boldsymbol{M}_1) \dot{-} \mathcal{W}(\boldsymbol{M}_2) \end{aligned}$$

Because permutation only changes pixel locations with their values unmodified, the pixels in the same positions are transferred to an identical coordinate in the ciphertexts, $\mathcal{W}(\boldsymbol{M}_1) \dot{-} \mathcal{W}(\boldsymbol{M}_2) = \mathcal{W}(\boldsymbol{M}_1 \dot{-} \boldsymbol{M}_2) = \mathcal{W}(\Delta\boldsymbol{M})$. Therefore,

$$\Delta\boldsymbol{C} = \mathcal{W}(\Delta\boldsymbol{M}). \tag{9}$$

Definition 1: The differential transfer function (DTF) $\mathcal{H}(\Delta\boldsymbol{M})$ is defined as the mapping from ΔM to ΔC in a certain encryption round, i.e.,

$$\Delta C = \mathcal{H}(\Delta\boldsymbol{M}).$$

Referring to Eq. (9), the DTF of the basic encryption scheme is

$$\Delta\boldsymbol{C} = \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}) = \mathcal{W}(\Delta\boldsymbol{M}). \tag{10}$$

Property 1: $\mathcal{H}_{(basic)}(\Delta\boldsymbol{M})$ has bijectivity, namely, $\Delta\boldsymbol{M}_1 = \Delta\boldsymbol{M}_2$if and only if$\mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_1) = \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_2)$.

Proof: The permutation operation $\mathcal{W}$ is a one-to-one mapping. Thus, $\mathcal{H}_{(basic)}(\Delta\boldsymbol{M}) = \mathcal{W}(\Delta\boldsymbol{M})$ is a bijection. The proof is completed. ■

Property 2: $\mathcal{H}_{(basic)}(\Delta\boldsymbol{M})$ has modular additivity, that is,

$$\begin{aligned} &\mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_1) \dot{+} \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_2) \\ &\quad = \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_1 \dot{+} \Delta\boldsymbol{M}_2). \end{aligned}$$

Proof: Considering that the permutation contributes only to pixel relocation and that the plain pixels in the same coordinates are shuffled to an identical position in the ciphertexts,

$$\begin{aligned} \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_1) \dot{+} \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_2) &= \mathcal{W}(\Delta\boldsymbol{M}_1) \dot{+} \mathcal{W}(\Delta\boldsymbol{M}_2) \\ &= \mathcal{W}(\Delta\boldsymbol{M}_1 \dot{+} \Delta\boldsymbol{M}_2) \\ &= \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}_1 \dot{+} \Delta\boldsymbol{M}_2) \end{aligned}.$$

End of proof. ■

Property 3: $\mathcal{H}_{(basic)}(\Delta\boldsymbol{M})$ has modular multiplicability, that is,

$$\lambda \dot{\times} \mathcal{H}_{(basic)}(\Delta\boldsymbol{M}) = \mathcal{H}_{(basic)}(\lambda \dot{\times} \Delta\boldsymbol{M}).$$

[5]For simplifying the following analysis, $w(i)$ here is essentially defined as the inverse of that in [27]–[29].

Proof: Because only pixel relocation is performed in the permutation phase,

$$\begin{aligned}\lambda \dot{\times} \mathcal{H}_{(basic)}(\Delta \boldsymbol{M}) &= \lambda \dot{\times} \mathcal{W}(\Delta \boldsymbol{M}) \\ &= \mathcal{W}(\lambda \dot{\times} \Delta \boldsymbol{M}) \\ &= \mathcal{H}_{(basic)}(\lambda \dot{\times} \Delta \boldsymbol{M}).\end{aligned}$$

End of proof. ■

Specifically, $\mathcal{H}^{(i)}_{(basic)}(\Delta \boldsymbol{M}^{(i)})$ denotes the DTF in the i^{th} encryption round. As indicated in Eq. (10), if different permutation vectors are used in different encryption rounds, $\mathcal{H}^{(i)}_{(basic)}(\Delta \boldsymbol{M}^{(i)})$ are also different from each other. However, all of them have bijectivity, modular additivity and modular multiplicative properties. In summary, the differential transfer functions $\mathcal{H}^{(i)}_{(basic)}(\Delta \boldsymbol{M}^{(i)})$ are key-dependent, whereas their bijectivity, modular additivity and modular multiplicability properties are key-independent.

Definition 2: The cascaded differential transfer function (CDTF) $\mathcal{H}^{(1)-(N)}(\Delta \boldsymbol{M}^{(1)})$ is defined as the mapping from the differential of the input plaintexts, i.e., $\Delta M^{(1)}$, to that of the output ciphertexts in the N^{th} encryption round, i.e., $\Delta C^{(N)}$, that is,

$$\Delta C^{(N)} = \mathcal{H}^{(1)-(N)}_{(cipher)}(\Delta \boldsymbol{M}^{(1)}). \tag{11}$$

Property 4: $\mathcal{H}^{(1)-(N)}_{(basic)}(\Delta \boldsymbol{M}^{(1)})$ also has bijectivity, modular additivity and modular multiplicability properties.

Proof: The proof is given in Appendix A. ■

Remark 1: For the basic encryption scheme, the differential of the output ciphertexts is $\Delta C^{(N)}$, which is correlated with the differential of the original plaintexts $\Delta \boldsymbol{M}^{(1)}$ as

$$\Delta C^{(N)} = \mathcal{H}^{(1)-(N)}_{(basic)}(\Delta \boldsymbol{M}^{(1)})$$

which is a bijective, modular additive and modular multiplicable function.

Hereinafter, the bijectivity, modular additivity and modular multiplicability are abbreviated as BAM properties.

C. The Proposed Chosen-Ciphertext Attack

The chosen-ciphertext attack is employed in this work. Specifically, arbitrary numbers of ciphertexts and their plaintexts are obtainable. By exploiting the knowledge residing in these ciphertext-plaintext pairs, the attack is said to be successful if any of the received ciphertext can be successfully recovered without the key. Note that for each studied image encryption scheme, it may also be vulnerable to other types of attacks. However, this work focuses on the common vulnerability of a family of image encryption schemes and proposes a universal chosen-ciphertext attack to break all these encryption schemes.

As demonstrated in Remark 1, the CDTF of the basic encryption scheme has BAM properties. Benefiting from these properties, a chosen-ciphertext attack is created to recover the plaintext. The proposed chosen-ciphertext attack is abbreviated as PCCA hereinafter. Algorithm 1 can be referenced for code implementation of PCCA. There are five steps, as described as follows.

1) Construct $L+1$ chosen-ciphertexts, where L refers to the pixel counts of the ciphertext. They are denoted as $\boldsymbol{C}_0^{(N)}, \boldsymbol{C}_1^{(N)}, \ldots, \boldsymbol{C}_i^{(N)}, \ldots, \boldsymbol{C}_L^{(N)}$. The ciphertext $\boldsymbol{C}_0^{(N)}$ is an all-zero image, while $\boldsymbol{C}_i^{(N)}, i \in [1, L]$ is constructed by

$$c_i^{(N)}(j) = \begin{cases} 1, j = i \\ 0, j \neq i, j \in [1, L] \end{cases}. \tag{12}$$

2) Obtain their corresponding plaintexts, represented as $\boldsymbol{M}_0^{(1)}, \boldsymbol{M}_1^{(1)}, \ldots, \boldsymbol{M}_i^{(1)}, \ldots, \boldsymbol{M}_L^{(1)}$.
3) Calculate the differentials of the plaintexts, i.e., $\Delta \boldsymbol{M}_i^{(1)} = \boldsymbol{M}_i^{(1)} \dot{-} \boldsymbol{M}_0^{(1)}, i \in [1, L]$. The plaintext $\boldsymbol{M}_0^{(1)}$ and the differentials $\Delta \boldsymbol{M}_1^{(1)}, \cdots \Delta \boldsymbol{M}_L^{(1)}$ jointly serve as the atoms that are used in steps 4 and 5.
4) For any eavesdropped ciphertext $\boldsymbol{C}^{(N)} = \{c^{(N)}(i), i \in [1, L]\}$, assume its plaintext as $\boldsymbol{M}^{(1)}$. Its differential between $\boldsymbol{M}_0^{(1)}$ is denoted as $\Delta \boldsymbol{M}^{(1)}$, which can be obtained according to

$$\Delta \boldsymbol{M}^{(1)} = \dot{\sum_{i=1}^{L}} [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{M}_i^{(1)}]. \tag{13}$$

- It is obvious that $\boldsymbol{C}^{(N)} = \dot{\sum}_{i=1}^{L} [c^{(N)}(i) \dot{\times} \boldsymbol{C}_i^{(N)}]$.
- Since $\boldsymbol{C}_0^{(N)}$ is an all-zero image, $\Delta \boldsymbol{C}_i^{(N)} = \boldsymbol{C}_i^{(N)} \dot{-} \boldsymbol{C}_0^{(N)} = \boldsymbol{C}_i^{(N)}$.
- Further, $\Delta \boldsymbol{C}^{(N)} = \dot{\sum}_{i=1}^{L} [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{C}_i^{(N)}]$.
- Referring to the CDTF's bijectivity, modular additivity and modular multiplicability, $\Delta \boldsymbol{M}^{(1)} = \dot{\sum}_{i=1}^{L} [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{M}_i^{(1)}]$.

Algorithm 1: The Proposed Chosen-Ciphertext Attack

Input: A ciphertext $\boldsymbol{C}^{(N)}$
Output: The plaintext $\boldsymbol{M}^{(1)}$ of $\boldsymbol{C}^{(N)}$

$L = Length(\boldsymbol{C}^{(N)})$;
$\boldsymbol{C}_0^{(N)} = zeros(1, L)$; // step 1: the first chosen-ciphertext
$\boldsymbol{M}_0^{(1)} = decrypt(\boldsymbol{C}_0^{(N)})$;
// decryption is feasible in a chosen-ciphertext attack
for each $i \in [1, L]$ **do**
$\boldsymbol{C}_i^{(N)} = zeros(1, L)$;
$c_i^{(N)}(i) = 1$;
// step 1: get other chosen-ciphertexts with Eq. (12)
$\boldsymbol{M}_i^{(1)} = decrypt(\boldsymbol{C}_i^{(N)})$; // step 2: obtain the plaintexts
$\Delta \boldsymbol{M}_i^{(1)} = \boldsymbol{M}_i^{(1)} \dot{-} \boldsymbol{M}_0^{(1)}$; // step 3: obtain the differentials
end for
$\Delta \boldsymbol{M}^{(1)} = zeros(1, L)$;
for each $i \in [1, L]$ **do**
$\Delta \boldsymbol{M}^{(1)} = \Delta \boldsymbol{M}^{(1)} \dot{+} c^{(N)}(i) \dot{\times} \Delta \boldsymbol{M}_i^{(1)}$;
// step 4: differential of the plaintext using Eq. (13)
end for
$\boldsymbol{M}^{(1)} = \Delta \boldsymbol{M}^{(1)} \dot{+} \boldsymbol{M}_0^{(1)}$; // step 5: recovery with Eq. (14)
return $\boldsymbol{M}^{(1)}$;

TABLE II
COMPARISON OF SOME CRYPTANALYSIS ACHIEVEMENTS

Cryptanalysis	Applicable image encryption scheme			Universality
	Permutation	Substitution	Iteration	
Xie *et al.* [22]	√	√	√	×
Solar *et al.* [23]	√	√	√	×
Wang *et al.* [24]	√	√	√	×
Wang *et al.* [25]	√	√	√	×
Li *et al.* [26]	√	√	×	×
Li *et al.* [27]	√	×	√	√
Li *et al.* [28]	√	×	√	√
Jolfaei *et al.* [29]	√	×	√	√
Zhang *et al.* [30]	×	√	√	√
Zhang *et al.* [35]	√	√	×	√
The proposed cryptanalysis	√	√	√	√

5) Finally, recover the plaintext $\boldsymbol{M}^{(1)}$ according to

$$\boldsymbol{M}^{(1)} = \Delta\boldsymbol{M}^{(1)} \dot{+} \boldsymbol{M}_0^{(1)}. \tag{14}$$

D. Universality and Discussions

As indicated in Section III-C, the CDTF's BAM properties essentially render the feasibility of PCCA. In addition, Property 4 reveals that if an encryption scheme's DTF has BAM features, its CDTF also has BAM properties. In summary, if an encryption scheme's DTF or CDTF has BAM properties, it is vulnerable to PCCA. The DTFs or CDTFs of a family of image encryption schemes are found to possess BAM properties, and PCCA is hence feasible for cracking them directly. In the literature, the image encryption schemes in [10]–[12], [14], [19], [31]–[34] fall within the scope of this work. Essentially, they are variants of the basic encryption model. The PCCA is feasible for breaking all of them without any modification.

In other words, the PCCA is applicable for breaking a family of image encryption schemes, rather than a specified scheme. In addition, the target image encryption schemes [10]–[12], [14], [19], [31]–[34] include both the permutation and substitution procedures, and the permutation-substitution network is allowed to iterate. However, there are some limitations in peer cryptanalysis works. Table II compares the proposed cryptanalysis with its counterparts. The attacks proposed in [22]–[26] are only feasible for their corresponding target encryption schemes, and they cannot break any other encryption schemes. The generalized attacks in [27]–[29] are limited to permutation-only encryption schemes, while Zhang *et al.* [30] focuses on substitution-only encryption schemes. This work first cryptanalyzes a family of image encryption schemes with iterative permutation-substitution networks.

In addition, the PCCA's complexity is independent of the encryption rounds and round keys. Referring to steps 1) – 3), PCCA needs $L+1$ chosen-ciphertexts to construct the atoms, i.e., $\boldsymbol{M}_0^{(1)}$ and $\Delta\boldsymbol{M}_i^{(1)}$. Once the atoms are established, any of the received ciphertexts can be straightforwardly cracked. The recovery process requires L modular addition and modular multiplication operations to calculate $\Delta\boldsymbol{M}^{(1)}$, while another modular addition is sufficient for constructing the plaintext. To conclude, the spatial and computational complexity of PCCA are both $O(L)$. It should be emphasized that the cost is independent of the encryption rounds N. This is counterintuitive compared with most cryptanalysis achievements whose complexity dramatically increases with the encryption rounds, such as the attack proposed in [23].

The security analysis in Section III-B straightforwardly indicates that the BAM properties of the CDTF of an image encryption scheme are independent of the employed nonlinear dynamics, permutation techniques, encryption rounds and round keys. As mentioned above, if an image encryption scheme's CDTF has BAM properties, it is vulnerable to PCCA. In other words, because the improvements in terms of complex nonlinear dynamics, novel permutation techniques, increasing encryption rounds and using round keys cannot change the CDTF's BAM properties; these types of enhancements are consequently infeasible to promote security against PCCA. The following sections further demonstrate that introducing previous ciphertexts for avalanches (Eqs. (2) and (3)) and inserting random pixels before the permutation-substitution network [12], [34] are also useless for improving an image encryption scheme's security against PCCA.

The success of AES has proven the security of the permutation-substitution framework and linear permutation for designing encryption schemes. Regarding the studied image encryption schemes, both the permutation and substitution (modular addition) are linear components, and the whole scheme is finalized into a linear cryptosystem. The proposed attack is thus feasible. For security enhancement, nonlinear substitution is strongly recommended for collaborating with the permutation module. As adopted in AES, substitution with a lookup table is highly suggested. In addition, mixing modular addition with the bitwise XOR [4] is also a candidate, but it must be repeated many times [35].

IV. APPLICATIONS TO THE STUDIED IMAGE ENCRYPTION SCHEMES

In this section, the PCCA is demonstrated to be applicable for breaking a family of image encryption schemes.

TABLE III
THE STUDIED IMAGE ENCRYPTION SCHEMES

Encryption schemes	Encryption process	Primary innovation	Applicable
ICS-IE [10]	1) key-dependent permutation 2) substitution with $k(i)\dot{-}m(i)$ 3) four iterations	1) a new integrated chaotic map 2) a permutation approach	yes
IE-PNG [31]	1) key-dependent permutation 2) substitution using Eq. (1)	a new permutation method	yes
TL-DEA [11]	1) substitution using Eq. (3) 2) key-dependent permutation 3) two iterations	1) a new cascade chaotic map 2) a permutation approach	yes
MIE-MA [12]	1) insert random pixels around the plaintext's four edges 2) key-dependent permutation 3) substitution using Eq. (2) 4) two iterations	1) inserting random pixels before permutation-substitution network 2) a fast permutation method	yes
LSCM-IEA [32]	1) key-dependent permutation 2) substitution using Eq. (3) 3) four iterations	1) a new coupling chaotic map 2) a new permutation method	yes
CMT-IEA [14]	1) key-dependent permutation 2) row-by-row and then column-by-column substitution using Eq. (2) 3) two iterations	1) a new coupling chaotic map 2) a new permutation method 3) two stages of substitution	yes
LSC-IES [19]	1) key-dependent permutation 2) rotation 3) substitution in random order using Eq. (2) 4) four iterations	1) a new coupling chaotic map 2) a new permutation method 3) the substitution is in random order	yes
IES-JPFD [33]	1) key-dependent permutation 2) substitution using image filtering, i.e., linking many neighbor pixels 3) two iterations	1) a new permutation method 2) substitution using image filtering	yes
IC-BSIF [34]	1) insert random pixels around two edges 2) key-dependent permutation 3) substitution using image filtering 3) four iterations	1) inserting random pixels before permutation-substitution network 2) substitution using image filtering 3) a new permutation method	yes

A. The Studied Image Encryption Schemes

Specifically, the studied image encryption schemes are the ICS-IE (integrated chaotic systems image encryption) [10], TL-DEA (tent-logistic map-based data encryption algorithm) [11], MIE-MA (medical image encryption using modulo arithmetic) [12], IE-PNG (image encryption using pseudorandom number generator);[6] [31], LSCM-IEA (2D-logistic-sine-coupling map-based image encryption algorithm) [32], CMT-IEA (chaotic magic transform-based image encryption algorithm) [14], LSC-IES (logistic-sine-cosine map-based image encryption scheme) [19], IES-JPFD (image encryption scheme utilizing Josephus problem and filtering diffusion) [33] and IC-BSIF (image cipher using block-based scrambling and image filtering) [34]. Compared with the basic encryption model described in Section III-A, the innovations are listed in Table III and categorized as follows.

1) All of the studied image encryption schemes had their own permutation techniques.
2) Some of the schemes [10], [11], [14], [19], [32] employed new chaotic maps for generating the permutation vectors and substitution masks.
3) Some of the schemes [11], [12], [14], [19], [32]–[34] introduced the previous ciphertexts into the current substitution, i.e., Eqs. (2) and (3) to obtain the avalanche effect.
4) Some of the schemes [12], [34] inserted random pixels before the permutation-substitution network to obtain resistance against plaintext attacks.

As a representative case, TL-DEA [11] is first employed to show that introducing previous ciphertexts into the current substitution is useless for resisting PCCA. MIE-MA [12] is subsequently taken as another example to reveal that inserting random pixels before core encryption is infeasible for resisting PCCA either. On this basis, attacks of other image encryption schemes [10], [14], [19], [31]–[34] are browsed. Because their innovations use new permutation techniques or chaotic maps, in comparison with the basic encryption model or the TL-DEA and MIE-MA, in Section III-D, these types of improvements have been revealed as useless for resisting PCCA.

B. Applicability to TL-DEA [11]

The substitution of TL-DEA is performed with Eq. (3). Therefore, a pixel's modification links with two previous ciphered pixels. The avalanche effect is thus obtained. It is taken as an example to show that substitution linking with other ciphered

[6]This encryption scheme has no abbreviation in [31] for easing the following analysis, it is named IE-PNG in this paper.

pixels is useless for resisting PCCA. The encryption processes of TL-DEA are as follows.

1) *Initialization:* The permutation vector W and substitution mask matrix K are generated with the key $Seed$ and cascade chaotic systems.
2) *Substitution:* The plain pixels are first substituted. Two previous ciphered pixels are linked for the avalanche effect, and the substitution ciphertext D is thus obtained as

$$d(i)=\begin{cases} m(i) \dot{+} k(i) \dot{+} m(L) \dot{+} m(L-1) & i=1 \\ m(i) \dot{+} k(i) \dot{+} d(i-1) \dot{+} m(L) & i=2 \\ m(i) \dot{+} k(i) \dot{+} d(i-1) \dot{+} d(i-2) & i \in [3, L] \end{cases}. \tag{15}$$

3) *Permutation:* The substitution ciphertext D is shuffled with W and a cycle permutation technique. Similarly, the permutation is finalized as Eq. (16).

$$\boldsymbol{C} = \mathcal{W}(\boldsymbol{D}). \tag{16}$$

4) *Iteration:* The above procedures are repeated twice with different $\boldsymbol{W}$ and $\boldsymbol{K}$ in each round.

Assume that there are two plaintexts $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$, their intermediate substitution results $\boldsymbol{D}_1$ and $\boldsymbol{D}_2$, and the ciphertexts $\boldsymbol{C}_1$ and $\boldsymbol{C}_2$ in a certain encryption round. It is obvious that

$$\Delta \boldsymbol{C} = \boldsymbol{C}_1 \dot{-} \boldsymbol{C}_2 = \mathcal{W}(\boldsymbol{D}_1) \dot{-} \mathcal{W}(\boldsymbol{D}_2) = \mathcal{W}(\boldsymbol{D}_1 \dot{-} \boldsymbol{D}_2) = \mathcal{W}(\Delta \boldsymbol{D}). \tag{17}$$

It is easy to rewrite the substitution (Eq. (15)) as

$$d(i) = \dot{\sum_{j=1}^{i}} Fib(i-j+1) \dot{\times} [m(j) \dot{+} k(j)] \dot{+} Fib(i+1) \dot{\times} m(L) \dot{+} Fib(i) \dot{\times} m(L-1)$$

where $Fib(i)$ represents the i^{th} particle of a Fibonacci sequence. Therefore,

$$\Delta d(i) = \dot{\sum_{j=1}^{i}} Fib(i-j+1) \dot{\times} \Delta m(j) \dot{+} Fib(i+1) \dot{\times} \Delta m(L) \dot{+} Fib(i) \dot{\times} \Delta m(L-1). \tag{18}$$

Combining Eqs. (17) and (18), TL-DEA's DTF is

$$\begin{cases} \Delta \boldsymbol{C} = \mathcal{H}_{(TL-DEA)}(\Delta \boldsymbol{M}) = \mathcal{W}(\Delta D) \\ \Delta d(i) = \dot{\sum_{j=1}^{i}} Fib(i-j+1) \dot{\times} \Delta m(j) \\ \qquad \dot{+} Fib(i+1) \dot{\times} \Delta m(L) \dot{+} Fib(i) \dot{\times} \Delta m(L-1) \end{cases}. \tag{19}$$

It is not difficult to obtain the BAM properties of $\mathcal{H}_{(TL-DEA)}(\Delta \boldsymbol{M})$.

1) *Bijectivity:* Referring to Eq. (19), it is obvious that the mapping from $\Delta \boldsymbol{M}$ to ΔD is revisable, while $\mathcal{W}$ also gives a bijection from ΔD to $\Delta \boldsymbol{C}$ in Eq. (17). Therefore, the mapping between $\Delta \boldsymbol{C}$ and $\Delta \boldsymbol{M}$, i.e., $\Delta \boldsymbol{C} = \mathcal{H}_{(TL-DEA)}(\Delta \boldsymbol{M})$, is bijective.
2) *Modular additivity and modular multiplicability:* As can be observed, $\mathcal{H}_{(TL-DEA)}(\Delta \boldsymbol{M})$ is a combination of permutation, modular addition and modular multiplication operations. All of them are apparently modular additives and modular multiplicables. As a consequence, $\mathcal{H}_{(TL-DEA)}(\Delta \boldsymbol{M})$ has modular additivity and modular multiplicability.

To conclude, $\mathcal{H}_{(TL-DEA)}(\Delta \boldsymbol{M})$ has BAM properties, and thus, TL-DEA is vulnerable to PCCA.

C. Applicability to MIE-MA [12]

The MIE-MA is proposed by Hua *et al.* [12].[7] Unlike most of the counterparts, MIE-MA first adds some random pixels around the plaintext and then encrypts the enlarged image by the permutation-substitution network. The insertion of random pixels makes the encryption scheme indistinguishable for resisting known-plaintext and chosen-plaintext attacks. To some extent, MIE-MA is introduced with specific motivation to show that such a random insertion process is infeasible for resisting PCCA. The encryption processes of MIE-MA are sketched as follows.

1) *Initialization:* With the key and logistic-sine map, generate the permutation vector W and substitution mask K.
2) *Random pixel insertion:* Generate $2 \times M + 2 \times N + 4$ random pixels and then paste them around the four sides of the input plaintext $\boldsymbol{M}$. Hence, an enlarged image $\boldsymbol{MI}$ with size $(H+2) \times (W+2)$ is produced.
3) *Permutation:* Shuffle the enlarged image $\boldsymbol{MI}$ using W and a row/column swapping approach. Analogously, the permutation procedure is generalized as

$$P = \mathcal{W}(\boldsymbol{MI}).$$

4) *Substitution:* Stretch P column by column, and then perform pixel substitution according to Eq. (20). Note that $L = (H+2) \times (W+2)$ in Eq. (20), refers to the total pixel counts in the ciphertext. As indicated, a previous ciphered pixel is linked.

$$c(i) = \begin{cases} p(i) \dot{+} k(i) \dot{+} p(L) & i=1 \\ p(i) \dot{+} k(i) \dot{+} c(i-1) & i \in [2, L] \end{cases}. \tag{20}$$

5) *Iteration:* Repeat the permutation-substitution network twice, using independent W and K.

Without loss of generality, the random inserted variables are denoted as $\boldsymbol{R}$, and the symbol $||$ is employed to denote the pixel insertion process. That means,

$$\boldsymbol{MI}^{(1)} = \boldsymbol{M}^{(1)} || \boldsymbol{R}. \tag{21}$$

Essentially, $\boldsymbol{MI}^{(1)}$ is the input of the permutation-substitution network, and it also denotes the decryption result before removing the edge pixels. Note that $\boldsymbol{R}$ is randomly generated in the encryption process; it is random and unobtainable when encrypting a plaintext. With respect to the decryption, these inserted pixels are recovered, and they are not random but definite. Therefore, $\boldsymbol{MI}^{(1)}$.

[7]Two image encryption schemes are proposed in [12] this paper focuses on MIE-MA, which uses modular addition for pixel substitution.

Since $\boldsymbol{M}$ and $\boldsymbol{C}$ have different sizes, it is difficult to obtain $\mathcal{H}_{(MIE-MA)}(\Delta \boldsymbol{M})$ directly. The relationship between the differential of $\boldsymbol{MI}$ and that of the ciphertext $\boldsymbol{C}$ becomes an alternative. It is distinctively denoted as $\Delta \boldsymbol{C} = \mathcal{H}'_{(MIE-MA)}(\Delta \boldsymbol{MI})$, without loss of generality. First, it is easy to rewrite MIE-MA's substitution formula (Eq. (20)) as

$$c(i) = p(L) \dot{+} \dot{\sum}_{j=1}^{i} [p(j) \dot{+} k(j)], \tag{22}$$

where $P = \mathcal{W}(\boldsymbol{MI})$, i.e., the permutation ciphertext of the enlarged image. Referring to the deduction of $\mathcal{H}_{(basic)}(\Delta \boldsymbol{M})$ in Section III-B and taking Eqs. (6) and (22) into consideration, $\mathcal{H}'_{(MIE-MA)}(\Delta \boldsymbol{MI})$ is obtained as

$$\begin{cases} \Delta \boldsymbol{C} = \mathcal{H}'_{(MIE-MA)}(\Delta \boldsymbol{MI}) \\ \Delta c(i) = \Delta mi(w(L)) \dot{+} \dot{\sum}_{j=1}^{i} \Delta mi(w(j)) \end{cases} \tag{23}$$

where $w(j)$ is the j^{th} element of W. Similar to $\mathcal{H}_{(TL-DEA)}(\Delta \boldsymbol{M})$, $\mathcal{H}'_{(MIE-MA)}(\Delta \boldsymbol{MI})$ also consists of a series of permutation, modular addition and modular multiplication operations. Thus, it has BAM properties. Furthermore, $\mathcal{H}'^{(1)-(N)}_{(MIE-MA)}(\Delta \boldsymbol{MI}^{(1)})$ also has BAM properties. Following the PCCA steps in Section III-C, the plaintext is recovered as follows.

1) Referring to the first step of the attack, $L+1$ chosen-ciphertexts, i.e., $\boldsymbol{C}_0^{(N)}, \ldots, \boldsymbol{C}_L^{(N)}$, are first constructed; all of them are of size $(H+2) \times (W+2)$.
2) Subsequently, $L+1$ decryption results, $\boldsymbol{M}_0^{(1)}, \ldots, \boldsymbol{M}_L^{(1)}$, are also obtainable. However, their sizes are all $H \times W$.
3) Furthermore, the differentials of the plaintexts are calculated according to $\Delta \boldsymbol{M}_i^{(1)} = \boldsymbol{M}_i^{(1)} \dot{-} \boldsymbol{M}_0^{(1)}$, $i \in [1, L]$.
4) For any ciphertext $\boldsymbol{C}^{(N)} = \{c^{(N)}(i), i \in [1, L]\}$, assume its plaintext as $\boldsymbol{M}^{(1)}$. Its differential between $\boldsymbol{M}_0^{(1)}$, i.e., $\Delta \boldsymbol{M}^{(1)}$, is obtained by Eq. (24).

$$\Delta \boldsymbol{M}^{(1)} = \dot{\sum}_{i=1}^{L} [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{M}_i^{(1)}]. \tag{24}$$

   Please refer to Appendix B for the deduction.
5) Therefore, the plaintext is recovered as $\boldsymbol{M}^{(1)} = \Delta \boldsymbol{M}^{(1)} \dot{+} \boldsymbol{M}_0^{(1)}$.

D. Applicability to Other Image Encryption Schemes [10], [14], [19], [31]–[34]

Except for the aforementioned case studies, the image encryption schemes in [10], [14], [19], [31]–[34] have similar architectures. They are also vulnerable to PCCA.

1) *Applicability to ICS-IE [10]:* The ICS-IE is quite similar to the basic encryption model. Two integrated chaotic maps are employed, and a new permutation approach is developed. A slight difference is that the substitution is performed using modular subtraction, specifically, $c(i) = k(i) \dot{-} m(i)$. Referring to the security analysis of the basic model given in Section III-B, it is easy to obtain the BAM properties of ICS-IE's DTF. Thus, PCCA is feasible for cracking this encryption scheme.
2) *Applicability to IE-PNG [31]:* The permutation is performed at the pixel level, and the substitution is performed with Eq. (1). A logistic map, Tompkins-Paige algorithm and tent map are employed for generating the permutation vector and substitution masks. These encryption elements are independent of the plaintexts. The security analysis of the basic model described in Section III-B is straightforwardly transplantable for IE-PNG.
3) *Applicability to LSCM-IEA [32]:* This encryption scheme consists of four permutation-substitution iterations. The permutation is performed at the pixel level, while two previous ciphertexts are included in the substitution as given in Eq. (3). Referring to the analysis of TL-DEA in Section IV-B, LSCM-IEA is vulnerable to PCCA accordingly. The adopted novel permutation technique, logistic-sine-coupling map and more encryption rounds cannot promote resistance against PCCA.
4) *Applicability to CMT-IEA [14]:* This encryption scheme employs a sine-logistic modulation map for key scheduling and introduces Eq. (2) for pixel substitution. A permutation, joint row-by-row and column-by-column substitutions constitute the encryption core, which iterates twice. Essentially, the encryption loop can be regarded as a two-layer permutation-substitution operation, where the second permutation is a 90° clock rotation. Referring to the analysis of MIE-MA, it is easy to conclude that the CMT-IEA DTF is similar to Eq. (23) by replacing $\Delta \boldsymbol{MI}$ as $\Delta \boldsymbol{M}$.[8] Therefore, the DTF also has BAM properties, and the PCCA is applicable.
5) *Applicability to LSC-IES [19]:* A cosine-transform-based chaotic system is developed for key stream generation, while Eq. (2) is used for substitution. The encryption core, composed of a permutation, rotation and substitution, is repeated four times. The LSC-IES has two features. First, there is an image rotation module between the permutation and substitution procedures. Second, the substitution is performed in a secret order. By considering the secret-order substitution as a permutation-then-substitution (sequential) procedure, the encryption core becomes three permutations and one substitution procedure. A single permutation vector is also sufficient for synthesizing the three permutation modules; LSC-IES is hence relaxed as a permutation-substitution network. Similar to the analysis of MIE-MA, PCCA is also applicable.
6) *Applicability to IES-JPFD [33] and IC-BSIF [34]:* Both image encryption schemes outfit the iterative permutation-substitution structure, yet the substitution is derived from the image filtering concept. Technically, many neighboring pixels are linked for substitution. Referring to the analysis when linking one

[8] As mentioned above, the security analysis of MIE-MA [12] in Section IV-C is described to show that inserting random pixels during the encryption process cannot promote security.

or two adjacent pixels for substitution, i.e., analysis of TL-DEA and MIE-MA given in Sections IV-B and IV-C, the DTFs of IES-JPFD and IC-BSIF are also composed of some permutation, modular addition and modular multiplication operations. Accordingly, they also have BAM properties. The IES-JPFD and IC-BSIF are also vulnerable to PCCA.

V. Experimental Results

This section presents the experimental results. The proposed attack and all the studied encryption schemes are implemented in MATLAB 2018, and their source codes are open and available online.[9] Note that we wrote the source codes of the proposed chosen-ciphertext attack and some studied image encryption schemes (including the basic encryption model, ICS-IE, and IE-PNG). The source codes of other studied image encryption schemes were downloaded from the Internet and directly used to verify the feasibility of our attack algorithm.

A. Illustration Experiment

TL-DEA is first employed to illustrate the attack processes step by step. The plaintext is also assumed to have 9 pixels for favorable representation. Of course, any other size of plaintext can be chosen. With a secret key, Alice encrypts an image

$$\boldsymbol{M}^{(1)} = \{0, 15, 33, 47, 65, 165, 56, 96, 255\},$$

and obtains the ciphertext

$$\boldsymbol{C}^{(N)} = \{29, 67, 144, 143, 74, 127, 101, 24, 139\},$$

which is eavesdropped by Eve. Subsequently, Eve attempts to recover the plaintext without the secret key. Completely complying with the attack procedures given in Section III-C, the signal recovery processes are illustrated as follows.

1) Construct $9 + 1 = 10$ chosen-ciphertexts, which are denoted as $\boldsymbol{C}_0^{(N)}, \boldsymbol{C}_1^{(N)}, \ldots, \boldsymbol{C}_9^{(N)}$.

$$\begin{aligned}
\boldsymbol{C}_0^{(N)} &= \{0,0,0,0,0,0,0,0,0\}\\
\boldsymbol{C}_1^{(N)} &= \{1,0,0,0,0,0,0,0,0\}\\
\boldsymbol{C}_2^{(N)} &= \{0,1,0,0,0,0,0,0,0\}\\
\boldsymbol{C}_3^{(N)} &= \{0,0,1,0,0,0,0,0,0\}\\
\boldsymbol{C}_4^{(N)} &= \{0,0,0,1,0,0,0,0,0\}\\
\boldsymbol{C}_5^{(N)} &= \{0,0,0,0,1,0,0,0,0\}\\
\boldsymbol{C}_6^{(N)} &= \{0,0,0,0,0,1,0,0,0\}\\
\boldsymbol{C}_7^{(N)} &= \{0,0,0,0,0,0,1,0,0\}\\
\boldsymbol{C}_8^{(N)} &= \{0,0,0,0,0,0,0,1,0\}\\
\boldsymbol{C}_9^{(N)} &= \{0,0,0,0,0,0,0,0,1\}
\end{aligned}$$

2) Under the assumption of a chosen-ciphertext attack, their plaintexts are obtained as

$$\begin{aligned}
\boldsymbol{M}_0^{(1)} &= \{85,16,228,187,2,230,109,110,193\}\\
\boldsymbol{M}_1^{(1)} &= \{86,14,227,189,3,230,109,110,193\}\\
\boldsymbol{M}_2^{(1)} &= \{85,17,226,186,4,231,109,110,193\}\\
\boldsymbol{M}_3^{(1)} &= \{85,16,229,185,1,232,110,110,193\}\\
\boldsymbol{M}_4^{(1)} &= \{84,16,228,188,0,229,111,111,193\}\\
\boldsymbol{M}_5^{(1)} &= \{82,15,228,187,3,228,108,112,194\}\\
\boldsymbol{M}_6^{(1)} &= \{85,13,227,187,2,231,107,109,195\}\\
\boldsymbol{M}_7^{(1)} &= \{90,16,225,186,2,230,110,108,192\}\\
\boldsymbol{M}_8^{(1)} &= \{86,19,227,186,2,230,109,111,191\}\\
\boldsymbol{M}_9^{(1)} &= \{83,15,230,188,2,230,109,110,194\}
\end{aligned}$$

3) The differentials of the plaintexts are

$$\begin{aligned}
\Delta\boldsymbol{M}_1^{(1)} &= \boldsymbol{M}_1^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{1,254,255,2,1,0,0,0,0\}\\
\Delta\boldsymbol{M}_2^{(1)} &= \boldsymbol{M}_2^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{0,1,254,255,2,1,0,0,0\}\\
\Delta\boldsymbol{M}_3^{(1)} &= \boldsymbol{M}_3^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{0,0,1,254,255,2,1,0,0\}\\
\Delta\boldsymbol{M}_4^{(1)} &= \boldsymbol{M}_4^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{255,0,0,1,254,255,2,1,0\}\\
\Delta\boldsymbol{M}_5^{(1)} &= \boldsymbol{M}_5^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{253,255,0,0,1,254,\\
&\qquad 255,2,1\}\\
\Delta\boldsymbol{M}_6^{(1)} &= \boldsymbol{M}_6^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{0,253,255,0,0,1,254,\\
&\qquad 255,2\}\\
\Delta\boldsymbol{M}_7^{(1)} &= \boldsymbol{M}_7^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{5,0,253,255,0,0,1,\\
&\qquad 254,255\}\\
\Delta\boldsymbol{M}_8^{(1)} &= \boldsymbol{M}_8^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{1,3,255,255,0,0,0,1,254\}\\
\Delta\boldsymbol{M}_9^{(1)} &= \boldsymbol{M}_9^{(1)} \dot{-} \boldsymbol{M}_0^{(1)} = \{254,255,2,1,0,0,0,0,1\}
\end{aligned}$$

4) For the eavesdropped ciphertext $\boldsymbol{C}^{(N)} = \{29, 67, 144, 143, 74, 127, 101, 24, 139\}$, assume its plaintext as $\boldsymbol{M}^{(1)}$ whose differential between $\boldsymbol{M}_0^{(1)}$ is further denoted as $\Delta\boldsymbol{M}^{(1)}$. Eve can obtain $\Delta\boldsymbol{M}^{(1)}$ through

$$\begin{aligned}
\Delta\boldsymbol{M}^{(1)} &= \dot{\sum_{i=1}^{9}} [c^{(N)}(i) \dot{\times} \Delta\boldsymbol{M}_i^{(1)}]\\
&= \{171,255,61,116,63,191,203,242,62\}
\end{aligned}$$

5) Finally, the plaintext $\boldsymbol{M}^{(1)}$ is recovered according to

$$\begin{aligned}
\boldsymbol{M}^{(1)} &= \Delta\boldsymbol{M}^{(1)} \dot{+} \boldsymbol{M}_0^{(1)}\\
&= \{171,255,61,116,63,191,203,242,62\}\\
&\quad \dot{+} \{85,16,228,187,2,230,109,110,193\}\\
&= \{0,15,33,47,65,165,56,96,255\}.
\end{aligned}$$

As can be observed, the recovered plaintext is exactly the same as Alice's original input $\boldsymbol{M}^{(1)}$.

B. Experimental Results

As mentioned above, the proposed attack is universal for a family of image encryption schemes. It is valid for breaking 9 image encryption schemes that are proposed in [10]–[12], [14], [19], [31]–[34], without any modification.

[9]The source codes can be found via https://github.com/lurenjia212/crack_modulo_addition

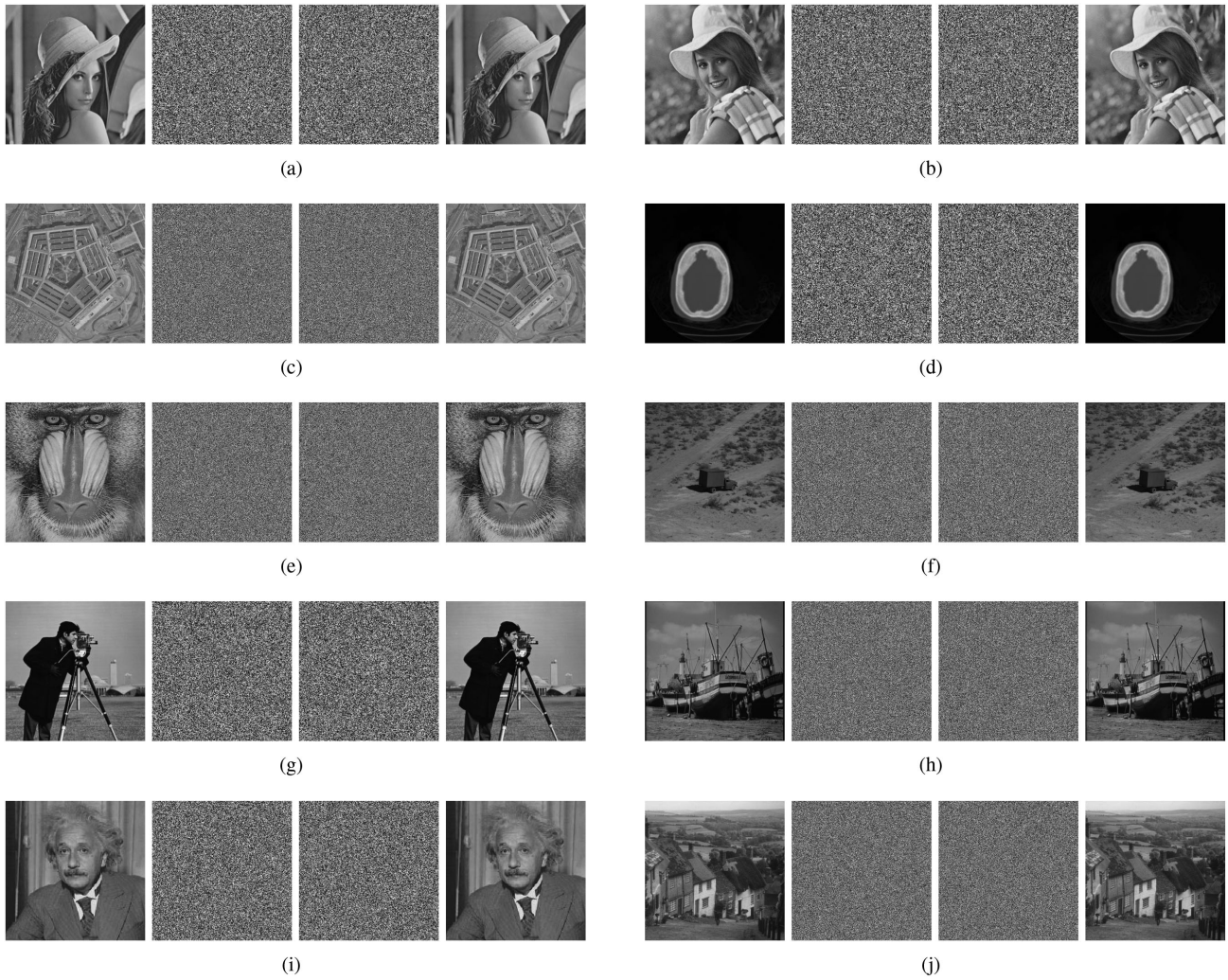


Fig. 2. Experimental results of the PCCA: (a) breaking the basic encryption scheme, plaintext is 256×256 lena.bmp; (b) breaking ICS-IE, plaintext is 256×256 elaine.png; (c) breaking TL-DEA, plaintext is 512×512 pentagon.tiff; (d) breaking MIE-MA, plaintext is a 256×256 CT image; (e) breaking IE-PNG, plaintext is 512×512 baboon.bmp; (f) breaking LSCM-IEA, plaintext is 512×512 truck.bmp; (g) breaking CMT-IEA, plaintext is 256×256 cameraman.bmp; (h) breaking LSC-IES, plaintext is 512×512 boat.bmp; (i) breaking IES-JPFD, plaintext is 283×283 einstein.png; and (j) breaking IC-BSIF, plaintext is 512×512 house.bmp. Four subsubfigures are included in each subfigure: the plaintext, ciphertext, differential between the plaintext with $\boldsymbol{M}_0$, and the recovered image.

Including the basic encryption model described in Section III-A, a total of 10 image encryption schemes are tested. The experimental results are demonstrated in Fig. 2. There are four subfigures in each suite of experimental results: plaintext, ciphertext, the retrieved differential between plaintext and $\boldsymbol{M}_0$, and the recovered image. The employed test images have different sizes and formats to evaluate the feasibility of PCCA comprehensively. The sizes and formats of the text images are illustrated in the caption of Fig. 2. With the full power of the chosen-ciphertext attack, the received ciphertexts can be attacked, and their plaintexts can be precisely recovered without the key. Numerical comparisons have proven the accuracy.

Theoretically, a chosen-ciphertext attack is available when the adversary can freely handle the decryption machine to obtain the required ciphertext-plaintext pairs. For the PCCA, $\boldsymbol{M}_0$ and $\Delta \boldsymbol{M}_i^{(1)}$ are the required ciphertext-plaintext pairs (atoms). When all of these atoms are available, the plaintext can be fully recovered, as shown in Fig. 2. If the decryption machine is only accessible for a short time, the adversary can only obtain part of the required ciphertext-plaintext bases. Some experiments are performed to evaluate the information leakage in this scenario. The IE-PNG is first analyzed. There is no avalanche effect in IE-PNG; thus, one pixel's recovery corresponds to the availability of a single atom. In contrast, if only some of the PCCA atoms are available, equal amounts of the plaintext may be recovered. When obtaining 10%, 50%, 90%, and 100% of the atoms, the recovered images are shown in Fig. 3. The accuracies are 10.38%, 50.23%, 90.08% and 100%, respectively. When the ratio of the required atoms ranges from 0 to 100%, the recovered image accuracies are plotted in Fig. 3(e). The accuracy linearly increases with the obtained atoms.

However, the relationship varies from the studied image encryption schemes. Considering CMT-IEA as an example, it uses Eq. (2) to change pixel values; thus, in an encryption round,

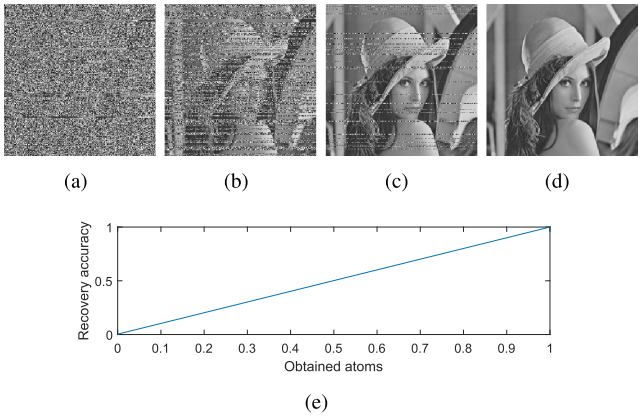


Fig. 3. Attacking IE-PNG using part of the atoms: (a) recovered image with 10% of the atoms; (b) recovered image with 50% of the atoms; (c) recovered image with 90% of the atoms; (d) recovered image with 100% of the atoms; (e) accuracy versus the obtained percentage of the atoms.

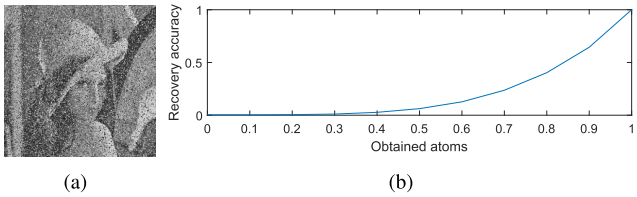


Fig. 4. Attacking CMT-IEA using part of the atoms: (a) recovered image with 90% of the atoms; (b) accuracy versus the obtained percentage of the atoms.

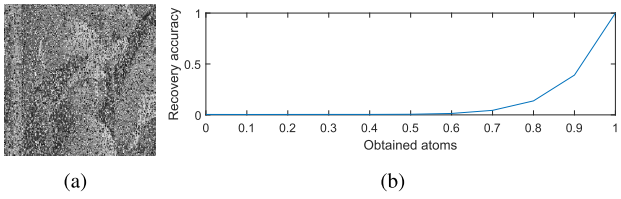


Fig. 5. Attacking TL-DEA using part of the atoms: (a) recovered image with 90% of the atoms; (b) accuracy versus the obtained percentage of the atoms.

the decryption (recovery) of a single pixel requires knowledge of two pixels. One pixel's information will affect two ciphered pixels' decryption. In addition, the permutation-substitution kernel repeats for two rounds in CMT-IEA. Therefore, if one atom is missing in PCCA, the recovery of four pixels may be influenced. Fig. 4(a) demonstrates the recovered images when 90% of the atoms are available, i.e., 10% of the atoms are unobtainable. A numerical comparison shows that 63.33% of the total pixels have been correctly recovered. The accuracy is lower than that of IE-PNG. Things become much worse when attacking TL-DEA, where a single ciphered pixel relates to two previous ciphered pixels. Therefore, the decryption (recovery) of a single pixel requires three pixels' knowledge in an encryption round. In addition, the permutation-substitution kernel iterates twice. When 10% of the atoms are missing, the recovered image is shown in Fig. 5(a). Compared with the plaintext, only 38.38% of the recovered pixels are correct. With different numbers of attack atoms, the accuracy curves of CMT-IEA and TL-DEA are quite different from that of IE-PNG. As revealed from Figs. 3(e), 4(b) and 5(b), missing equal numbers of atoms will create more incorrectness when attacking CMT-IEA and TL-DEA. In other words, it is more difficult to launch a chosen-ciphertext attack for CMT-IEA and TL-DEA. To some extent, this phenomenon also indicates that integrating diffusion (avalanche) effects into the substitution, and increasing encryption rounds can promote the security level. However, information leakage exists when encountering PCCA. With the full power of the chosen-ciphertext attack, i.e., all the required ciphertext-plaintext bases are obtainable, the plaintexts can be recovered exactly.

VI. Conclusion

This paper has evaluated the security of a family of image encryption schemes. Their permutation techniques were performed at the pixel level, while the substitutions were implemented by modular addition. The linearity between the differential of the plaintexts and that of the ciphertexts was first found. On that basis, a universal chosen-ciphertext attack was proposed that can decrypt the ciphertext without retrieving the secret key or equivalent encryption elements. It was also illustrated that some routine improvements, such as new dynamic systems and permutation techniques, could not remedy the reported security flaws. Potential attempts to develop similar image encryption schemes should be reconsidered. Future cryptanalysis works should focus on attacking the substitution method using mixed modular addition and bitwise XOR, while nonlinear substitution is highly suggested for inclusion in the design of image encryption schemes.

Appendix A
Proof of Property 4

For image encryption schemes with iterative architecture, the output in the $(i-1)^{th}$ layer is the input of the next encryption round, as shown in Eq. (8). Therefore,

$$\begin{aligned}\Delta \boldsymbol{C}^{(i)} &= \mathcal{H}^{(i)}_{(basic)}(\Delta \boldsymbol{M}^{(i)}) \\ &= \mathcal{H}^{(i)}_{(basic)}(\Delta \boldsymbol{C}^{(i-1)}) \\ &= \mathcal{H}^{(i)}_{(basic)}[\mathcal{H}^{(i-1)}_{(basic)}(\Delta \boldsymbol{C}^{(i-2)})] \\ &= \ldots \\ &= \mathcal{H}^{(i)}_{(basic)}\{\mathcal{H}^{(i-1)}_{(basic)}[\ldots \mathcal{H}^{(1)}_{(basic)}(\Delta \boldsymbol{C}^{(0)})]\} \\ &= \mathcal{H}^{(i)}_{(basic)}\{\mathcal{H}^{(i-1)}_{(basic)}[\ldots \mathcal{H}^{(1)}_{(basic)}(\Delta \boldsymbol{M}^{(1)})]\}. \end{aligned} \tag{25}$$

In other words,

$$\mathcal{H}^{(1)-(N)}_{(basic)}(\Delta \boldsymbol{M}^{(1)}) = \mathcal{H}^{(N)}_{(basic)}\{\mathcal{H}^{(N-1)}_{(basic)}[\ldots \mathcal{H}^{(1)}_{(basic)}(\Delta \boldsymbol{M}^{(1)})]\}.$$

Because $\mathcal{H}^{(i)}_{(basic)}(\Delta \boldsymbol{M}^{(i)}), i \in [1, N]$ is bijective, modular additive and modular multipliable, $\mathcal{H}^{(1)-(N)}_{(basic)}(\Delta \boldsymbol{M}^{(1)})$ consequently has the properties of bijectivity, modular additivity and modular multiplicability.

Hence, the proof is completed.

APPENDIX B
DEDUCTION OF EQ. (24)

In PCCA, only the output ciphertexts $\boldsymbol{C}_0^{(N)}, \ldots, \boldsymbol{C}_L^{(N)}$ and corresponding input plaintexts $\boldsymbol{M}_0^{(1)}, \ldots, \boldsymbol{M}_L^{(1)}$ are obtainable. As intermediate products in the decryption process, $\boldsymbol{MI}_0^{(1)}, \ldots, \boldsymbol{MI}_L^{(1)}$ and $\boldsymbol{R}_0, \ldots, \boldsymbol{R}_L$ exist at the end of the permutation-substitution network. In addition, there is no randomness in the decryption process, and a ciphertext $\boldsymbol{C}^{(N)}$ will definitely be decrypted into the corresponding $\boldsymbol{M}^{(1)}$. Thus, $\boldsymbol{MI}^{(1)}$ and $\boldsymbol{R}$ are also definite although unobtainable. According to Eq. (21), it is easy to obtain

$$\boldsymbol{MI}_i^{(1)} = \boldsymbol{M}_i^{(1)} || \boldsymbol{R}_i.$$

Further,

$$\Delta \boldsymbol{MI}_i^{(1)} = \boldsymbol{MI}_i^{(1)} \dot{-} \boldsymbol{MI}_0^{(1)} = (\boldsymbol{M}_i^{(1)} || \boldsymbol{R}_i) \dot{-} (\boldsymbol{M}_0^{(1)} || \boldsymbol{R}_0).$$

Since $||$ is a pixel-insertion operation and considering that pixels in different positions cannot affect each other in the modular subtraction ($\dot{-}$) of two pixels,

$$\begin{aligned}(\boldsymbol{M}_i^{(1)} || \boldsymbol{R}_i) \dot{-} (\boldsymbol{M}_0^{(1)} || \boldsymbol{R}_0) &= (\boldsymbol{M}_i^{(1)} \dot{-} \boldsymbol{M}_0^{(1)}) || (\boldsymbol{R}_i \dot{-} \boldsymbol{R}_0) \\ &= \Delta \boldsymbol{M}_i^{(1)} || \Delta \boldsymbol{R}_i.\end{aligned}$$

To be concluded,

$$\Delta \boldsymbol{MI}_i^{(1)} = \Delta \boldsymbol{M}_i^{(1)} || \Delta \boldsymbol{R}_i, \tag{26}$$

where $\Delta \boldsymbol{MI}_i$ and $\Delta \boldsymbol{R}_i$ are unknown but not random. For the plaintext awaiting for recovery, it is obvious that

$$\Delta \boldsymbol{MI}^{(1)} = \Delta \boldsymbol{M}^{(1)} || \Delta \boldsymbol{R}. \tag{27}$$

However, considering that $\mathcal{H}'^{(1)-(N)}_{(MIE-MA)}(\Delta \boldsymbol{MI}^{(1)})$ has BAM properties,

$$\Delta \boldsymbol{MI}^{(1)} = \dot{\sum_{i=1}^{L}} [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{MI}_i^{(1)}].$$

Referring to Eq. (26),

$$\begin{aligned}c^{(N)}(i) \dot{\times} \Delta \boldsymbol{MI}_i^{(1)} &= c^{(N)}(i) \dot{\times} (\Delta \boldsymbol{M}_i^{(1)} || \Delta \boldsymbol{R}_i) \\ &= [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{M}_i^{(1)}] || [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{R}_i]\end{aligned}$$

Therefore,

$$\begin{aligned}\Delta \boldsymbol{MI}^{(1)} &= \dot{\sum_{i=1}^{L}} [c^{(N)}(i) \dot{\times} \Delta \boldsymbol{MI}_i^{(1)}] \\ &= \dot{\sum_{i=1}^{L}} (c(i) \dot{\times} \Delta \boldsymbol{M}_i^{(1)}) || (c^{(N)}(i) \dot{\times} \Delta \boldsymbol{R}_i) \\ &= \dot{\sum_{i=1}^{L}} \{(c^{(N)}(i) \dot{\times} \Delta \boldsymbol{M}_i^{(1)})\} || \dot{\sum_{i=1}^{L}} \{(c(i) \dot{\times} \Delta \boldsymbol{R}_i)\}\end{aligned} \tag{28}$$

Comparing the left parts of $||$ in Eqs. (27) with (28), Eq. (24) consequently holds.

REFERENCES

[1] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystem," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[2] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inform. Forensics Secur.*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[3] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[4] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos Solitons Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[5] M. Zanin and A. N. Pisarchik, "Gray code permutation algorithm for high-dimensional data encryption," *Inf. Sci.*, vol. 270, pp. 288–297, 2014.

[6] J. A. E. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 3, pp. 578–588, 2014.

[7] M. Dzwonkowski, M. Papaj, and R. Rykaczewski, "A new quaternion-based encryption method for DICOM images," *IEEE Trans. Image Process.*, vol. 24, no. 11, pp. 4614–4622, Nov. 2015.

[8] P. Praveenkumar, K. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Triple chaotic image scrambling on RGB—A random image encryption approach," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 3335–3345, 2015.

[9] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[10] R. Lan, J. He, S. Wang, T. Gu, and X. Luo, "Integrated chaotic systems for image encryption," *Signal Process.*, vol. 147, pp. 133–145, 2018.

[11] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[12] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, 2018.

[13] Z. Lin, S. Yu, J. Lü, S. Cai, and G. Chen, "Design and arm-embedded implementation of a chaotic map-based real-time secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 25, no. 7, pp. 1203–1216, Jul. 2015.

[14] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, 2015.

[15] Y. Yang, Q. Pan, S. Sun, and P. Xu, "Novel image encryption based on quantum walks," *Scientific Rep.*, vol. 5, no. 1, pp. 7784–7784, 2015.

[16] M. Kaur and V. Kumar, "Efficient image encryption method based on improved Lorenz chaotic system," *Electron. Lett.*, vol. 54, no. 9, pp. 562–564, 2018.

[17] O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, and S. Belghith, "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity," *Nonlinear Dyn.*, vol. 82, no. 1, pp. 107–117, 2015.

[18] W.-H. Chen, S. Luo, and W. X. Zheng, "Impulsive synchronization of reaction-diffusion neural networks with mixed delays and its application to image encryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 12, pp. 2696–2710, Dec. 2016.

[19] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, 2019.

[20] A. A. A. El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073–1081, 2018.

[21] X. Wang and D. Xu, "A novel image encryption scheme based on Brownian motion and PWLCM chaotic system," *Nonlinear Dyn.*, vol. 75, no. 2, pp. 345–353, 2014.

[22] E. Y. Xie, C. Li, S. Yu, and J. Lu, "On the cryptanalysis of Fridrich's chaotic image encryption scheme," *Signal Process.*, vol. 132, pp. 150–154, 2017.

[23] E. Solak and O. T. Yildiz, "Cryptanalysis of Fridrich's chaotic image encryption," *Int. J. Bifurcation Chaos*, vol. 20, no. 5, pp. 1405–1413, 2010.

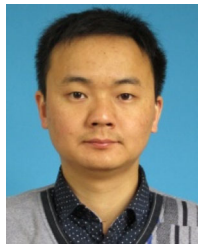
[24] L. Chen and S. Wang, "Differential cryptanalysis of a medical image cryptosystem with multiple rounds," *Comput. Biol. Med.*, vol. 65, pp. 69–75, 2015.

[25] L. Chen, B. Ma, X. Zhao, and S. Wang, "Differential cryptanalysis of a novel image encryption algorithm based on chaos and Line map," *Nonlinear Dyn.*, vol. 87, no. 3, pp. 1797–1807, 2017.

[26] M. Li, H. Fan, Y. Xiang, Y. Li, and Y. Zhang, "Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system," *IEEE Multimedia*, vol. 25, no. 3, pp. 92–101, Jul.–Sep. 2018.

[27] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K. Lo, "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Process.-Image Commun.*, vol. 23, no. 3, pp. 212–223, 2008.

[28] C. Li and K.-T. Lo, "Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Process.*, vol. 91, no. 4, pp. 949–954, 2011.
[29] A. Jolfaei, X. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 2, pp. 235–246, Feb. 2016.
[30] Y. Zhang and D. Xiao, "Cryptanalysis of S-box-only chaotic image ciphers against chosen plaintext attack," *Nonlinear Dyn.*, vol. 72, no. 4, pp. 751–756, 2013.
[31] S. E. Borujeni and M. Eshghi, "Chaotic image encryption design using Tompkins-Paige algorithm," *Math. Problems Eng.*, vol. 2009, pp. 1–22, 2009.
[32] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, 2018.
[33] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using josephus problem and filtering diffusion," *IEEE Access*, vol. 7, pp. 8660–8674, 2019.
[34] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, 2017.
[35] L. Y. Zhang *et al.*, "On the security of a class of diffusion mechanisms for image encryption," *IEEE Trans. Cybern.*, vol. 48, no. 4, pp. 1163–1175, Apr. 2018.
[36] F. Yu, X. Gong, H. Li, and X. Zhao, "Differential cryptanalysis of image cipher using block-based scrambling and image filtering," 2018, *arXiv:1812.11693*.
[37] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, 2018.
[38] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools Appl.*, vol. 75, no. 17, pp. 10 631–10 648, 2016.
[39] Z. Zhu, W. Zhang, K. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci.*, vol. 181, no. 6, pp. 1171–1186, 2011.
[40] J. He, S. Huang, S. Tang, and J. Huang, "JPEG image encryption with improved format compatibility and file size preservation," *IEEE Trans. Multimedia*, vol. 20, no. 10, pp. 2645–2658, Oct. 2018.
[41] P. Li and K.-T. Lo, "A content-adaptive joint image compression and encryption scheme," *IEEE Trans. Multimedia*, vol. 20, no. 8, pp. 1960–1972, Aug. 2018.
[42] X. Tong, "The novel bilateral-diffusion image encryption algorithm with dynamical compound chaos," *J. Syst. Softw.*, vol. 85, no. 4, pp. 850–858, 2012.
[43] H. Diab, "An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations," *IEEE Access*, vol. 6, pp. 42 227–42 244, 2018.
[44] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Opt. Lasers Eng.*, vol. 90, pp. 146–154, 2017.
[45] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools Appl.*, vol. 71, no. 3, pp. 1469–1497, 2014.
[46] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, 2019, Art. no. 102361.
[47] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Arch. Comput. Methods Eng.*, vol. 27, pp. 15–43, 2020.



Junxin Chen received the B.Sc., M.Sc., and Ph.D. degrees from Northeastern University, Shenyang, China, in 2007, 2009, and 2016 respectively, all in communications engineering. He is currently an Associate Professor with the College of Medicine and Biological Information Engineering, Northeastern University. He is also with the Department of Computer and Information Science, University of Macau, Macau SAR, China. He has authored or coauthored more than 50 scientific paper in peer-reviewed journals and conferences, including IEEE TRANSACTIONS OF INDUSTRIAL INFORMATICS, IEEE INTERNET OF THINGS JOURNAL, IEEE PHOTONICS JOURNAL, INFORMATION SCIENCES, etc. His research interests include biosignal processing, compressive sensing, security and privacy.

Lei Chen received the Ph.D. degree in electronic science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2018. He is currently a Postdoctoral Fellow with the Research Institute of Information Technology (RIIT), Tsinghua University, Beijing, China. He is also with Nsfocus Information Technology Company, Ltd., Beijing, China. His research interests include multimedia security, cryptanalysis, data security, and machine learning for cyberspace security.

Yicong Zhou (Senior Member, IEEE) received the B.S. degree from Hunan University, Changsha, China, and the M.S. and Ph.D. degrees from Tufts University, Medford, MA, USA, all in electrical engineering. He is currently an Associate Professor and the Director of the Vision and Image Processing Laboratory, Department of Computer and Information Science, University of Macau, Macau. His research interests include image processing, computer vision, machine learning, and multimedia security. Dr. Zhou is a Senior Member of the International Society for Optical Engineering (SPIE). He was the recipient of the Third Price of Macao Natural Science Award in 2014 and 2020. He is a Co-Chair of Technical Committee on Cognitive Computing in the IEEE Systems, Man, and Cybernetics Society. He serves as an Associate Editor for the IEEE TRANSACTIONS ON NEUTRAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, IEEE TRANSACTIONS ON GEOSCIENCE AND REMOTE SENSING, and four other journals.